DOI:10.1145/3072528 Bo Brinkman, Catherine Flick, Don Gotterbarn,[a] Keith Miller, Kate Vazansky, Marty J. Wolf

Listening to Professional Voices: Draft 2 of the ACM Code of Ethics and Professional Conduct

FOR THE FIRST time since 1992, the ACM Code of Ethics and Professional Conduct (the Code) is being updated. The Code Update Task Force in conjunction with the Committee on Professional Ethics is seeking advice from ACM members on the update. We indicated many of the motivations for changing the Code when we shared Draft 1 of Code 2018 with the ACM membership in the December 2016 issue of CACM[b] and with others through email and the COPE website (ethics.acm.org). Since December, we have been collecting feedback and are vetting proposed changes.

We have seen a broad range of concerns about responsible computing including bullying in social media, cyber security, and autonomous machines making ethically significant decisions. The Task Force appreciates the many serious and thoughtful comments it has received. In response, the Task Force has proposed changes that are reflected in Draft 2 of the Code. There are a number of substantial changes that require some explanation. In this article, we discuss these, and we explain why we did not include other requested changes in Draft 2. We look forward to receiving your comments on these suggested changes and your requests for additional changes as we work on Draft 3 of the Code. We have provided opportunities for your comments and an open discussion of Draft 2 at the ACM Code 2018 Discussion website [http://code2018.acm.org/discuss]. Comments can also be contributed at the COPE website https://ethics.acm.org, and by direct emails to chair@ethics.acm.org.

a Corresponding author and chair of Code 2018 project chair@ethics.acm.org

b http://cacm.acm.org/magazines/2016/12/210366-the-acm-code-of-ethics/fulltext

The Nature of an Ethics Code

ACM members are part of the computing profession and the ACM's Code of Ethics and Professional Conduct should reflect the conscience of the computing profession. When the Code adequately reflects the ethics of the profession, it also clarifies what that profession should strive to be. A code provides positive direction for its members.

The current update of the ACM Code begins positively; "Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing." As computing professionals, we are asked to promote good while working within ethical constraints including: be honest, don't cause harm, and avoid conflicts of interest. As the areas in which computing can make a positive impact have increased so has the range of our moral responsibility.

In Draft 1, the Task Force's suggested modifications reflected the need for members to better understand how computing technologies and artifacts impact the social infrastructure and how they ought to promote the common good. Professionalism in computing requires us to improve our abilities to anticipate broader impacts, both positive and negative, and to accept responsibility for those impacts.

This understanding of a code helps address concerns expressed by many commenters who noted a lack of clarity about to whom the ACM's Code applies. There were places where the Code seemed to apply to computing professionals more generally and other places where it seemed to apply only to ACM members. There were even a few places where the Code seemed to apply only to ACM members who were also computing professionals.

These concerns are addressed in Draft 2 in three ways. First, the Preamble now identifies what is meant by "computing professional." We intend for this term to be interpreted broadly, including students, software engineers, software architects, managers, leaders, and computer science teachers and scholars. Given the ubiquity of computing and the aspirational nature of the Code, we therefore aim to include those who may consider themselves professionals in the area of computing from non-standard backgrounds as well as those more traditionally considered computing professionals.

A second change intended to reflect that the Code provides aspirational guidance to a broad community involved replacing the categorical language of "moral imperatives" with the less prescriptive "ethical principles." Each of the principles in the Code is to be used to help us understand our ethical responsibility and to guide our decision making in varying and complex situations, rather than provide a rigid set of rules to follow unthinkingly. These principles are to be considered in our deliberations as we set professional goals for ourselves and carry out our daily activities. Section 1, especially, sets forth principles that need to be given special weight in those deliberations.

A third change was to clarify that every principle applies to computing professionals, regardless of their affiliation with the ACM, with the exception of the guidance given in Section 4. In principle 4.1, ACM members take on the additional responsibility of encouraging and supporting adherence to the ACM Code by all computing professionals. In the guidance for principle 4.2, we have retained the language whereby ACM members who violate the Code may have their membership terminated.

Requested Changes Made

One of the primary reasons for updating the Code is the increased influ-

ence of computing since 1992. Principle 1.1 has been modified to make this change (that almost all people are now impacted by computing) explicit by adding to the principle "acknowledging that all people are stakeholders in computing and its artifacts." The phrase "computing and its artifacts" is meant to remind practitioners that it is not just the code that they write that matters, but also those things that emerge from that code. In particular, the Task Force is addressing growing concerns about algorithms that emerge from machine learning rather than directly from algorithm designers. Consistent with the importance of computing and the ways it can contribute to society, we added an encouragement to perform pro bono or volunteer work. Like other professions, computing is a service to society. Following John Rawls' difference principle,[c] we emphasized computing professionals' responsibility toward the least powerful: "When the interest of multiple groups conflict, the needs of the least advantaged should be given increased attention and priority."

The revisions to principle 1.2 continue the clarification of a computing professional's responsibility to a broad range of stakeholders, and of the responsibility not to harm them. Sometimes causing harm is not unethical; examples often cited include self-defense and a just war. We have modified this principle to reflect these exceptions. Emergent technologies such as data remixing or policy-making software can also cause harm. To address this concern we have added, "Those involved with pervasive or infrastructure systems should also consider Principle 3.7" which advocates deeper analysis of emergent systems such as machine learning.

In the 1992 Code, principle 1.4 read "Be fair and take action not to discriminate." There was some concern that this might be misinterpreted due to the fact that "discrimination" does not necessarily imply unfairness, and in Draft 1 it was changed to "Be fair and take action not to discriminate *unfairly*." This has been roundly criticized as being even worse and may appear to some as a loophole for those who are seeking to justify discrimination that is unfair. Hence, in Draft 2, we have reverted back to the 1992 language.

Professionalism in computing requires us to improve our abilities to anticipate broader impacts, both positive and negative, and to accept responsibility for those impacts.

A frequent request was to explicitly address harassment, and especially sexual harassment, in the Code. The line "Sexual harassment is a form of discrimination that limits fair access to the spaces where the harassment takes place" has been added to the guidance of principle 1.4. The Task Force is attempting to correct a common misunderstanding about sexual harassment, the (false) belief that it does not have any consequences beyond just offending the harassed party. Instead, we emphasize that harassment is also a form of unfair discrimination because it makes the workplace or place of study unfairly inhospitable to certain individuals based on their identity. Sexual harassment is, in itself, an offense against principle 1.4 and other principles of the Code.

Principle 1.4 also speaks against bullying, a form of harassment based on a power differential rather than on sexual difference (although sexual harassment may also include power differentials). For example, it speaks against academic bullying which may occur when a more established scholar, or a person who has power because of their position (for example, an editor or program committee member), misuses that power to make unreasonable demands or to harm early career scholars, including graduate students. Bullying is also a form of unfair discrimination, as it does not recognize the inherent worth of every person and group.

In the 1992 Code, principles 1.5 and 1.6 were about honoring physical and intellectual property (IP) rights (copyright, patents, and crediting others' work). Draft 1 merged these to create a single statement about intellectual property rights. Understandably, the world of IP has changed significantly since 1992, and these days the definitions of "intellectual property" are complex and controversial, particularly in the computing world. Thus we received some significant criticism on the rewrite of this section, from multiple sides of intellec-

c Rawls, J. (2001) *Justice as Fairness: A Restatement*, E. Kelly (ed.), Cambridge, MA: Harvard University Press.

tual property arguments. The Task Force, after extensive discussion both internally and externally,[d] simplified the focus of this principle to a basic concept that the Code should protect the time, effort, and often considerable risk taken by people who come up with new ideas, innovations, and creative works; computing professionals should honor those investments. These creators usually have made decisions about how to protect their work; choices include open source or creative commons licensing, copyright, patents, other traditional legal avenues, or wanting no protection at all. This change also takes into account norms for specific endeavors, for example, the expectation that academic work will be cited if used in other research, teaching, or innovation. Since created works add significant value to society, the Code specifies that the creators' wishes for their works should be respected.

In moving away from explicitly listing in the Code the specific methods to be respected with respect to intellectual property works, we allow for a continuing dialogue on what the legal methods ought to be and focus on what computing professionals should do once a method is decided upon by the creator. We hope that computing professionals will be encouraged to investigate more open methods of sharing their works, with the full knowledge that the Code requires other professionals to respect their decisions about their works.

In addition to these requested changes, the Task Force made a number of smaller changes. For example, the guidance to principle 2.6 was shortened in order to add clarity. To further emphasize the importance of using the public good as the paramount decision-making principle, we moved principle 3.4 to principle 3.1, which resulted in the renumbering of principles 3.1, 3.2, and 3.3. We made further clarifying changes in principles 3.2, 3.3, and 3.4 to better reflect that leaders and groups in contemporary software development process are often more flexible and transient.

d The Task Force would like to thank Brian Ballsun-Stanton in particular for his feedback on an early redraft of this section.

Requested Changes Not Made

There were numerous requests for more specificity within the Code. Many commenters were looking for clear and specific definitions of terms like "harm" and "public good." Presumably, with more detailed definitions of these terms, there would be more clarity about applying the Code to specific situations. That is, the Code would become much more like an algorithm that would generate a clear indication of required action in specific situations. We decided against this request primarily for two reasons. The first is to reflect that society and social values are fluid. Our second reason stems from the fact that one of the responsibilities established in principle 2.2 is for the computing professional to maintain "skill in reflective analysis for recognizing and navigating ethical challenges." A computing professional who is maintaining such skill will quite naturally be in a position to understand these more fluid terms. Indeed, part of professional practice might include regular reflection on the nature of these terms.

Additionally, there were requests to incorporate into the Code explicit principles and guidance relating to specific forms of computing technology such as cyber security and artificial intelligence. While it is clear that these are areas of concern, they are beyond the scope of a code of ethics that is intended for the more broad definition of "computing professional" that we employ here. The particular ethical behaviors surrounding specific computing technologies are derivable from the general principles of the Code. For example, it follows from principle 2.5 that those working in AI should do a proactive analysis of the potential future impacts of self-mutating code. Nonetheless, COPE is planning on developing supporting materials that will illustrate how these broad principles apply to specific technologies. In our experience, changing supporting materials is far easier than changing the Code, so this strategy should help the ACM to be more agile in reacting to the ethical implications of new applications of technology.

Finally, there were also requests for including a compliance policy in the Code. The Task Force has chosen to approach compliance in a different way. The Code is something that can be used by all computing professionals regardless of their affiliation with the ACM, but compliance issues are limited to ACM members and ACM events. Therefore, aside from the broad principles in Section 4, compliance procedures will be in the ACM bylaws, not in the Code itself. COPE is cooperating with the ACM Council to develop a new compliance policy that better supports enforcement of the Code. We plan to include in those policies appropriate due process procedures, and multiple levels of sanctions to better reflect that some violations of the Code are more serious than others.

We invite further suggestions on issues that COPE might consider for future revisions. They can be submitted at the ACM Code 2018 Discussion website (http://code2018.acm.org/discuss) We look forward to receiving your comments for improving the Code.

ACM Code of Ethics and Professional Conduct: Draft 2

Draft 2 was developed by The Code 2018 Task Force. (It is based on the 2018 ACM Code of Ethics and Professional Conduct: Draft 1).[e]

Preamble

The ACM Code of Ethics and Professional Conduct ("the Code") identifies key elements of ethical conduct in computing.

The Code is designed to support all computing professionals, which is taken to mean current or aspiring computing practitioners as well as those who influence their professional development, and those who use technology in an impactful way. The Code includes principles formulated as statements of responsibility, based on the understanding that the public good is always a primary consideration. Section 1 outlines fundamental ethical considerations. Section 2 addresses additional, more

e A complete track changes version of Draft 2 showing all additions and deletions to Draft 1 version is available at http://ethics.acm.org/code-2018.

specific considerations of professional responsibility. Section 3 pertains more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer professional capacity. Commitment to ethical conduct is required of every ACM member and principles involving compliance with the Code are given in Section 4.

The Code as a whole is concerned with how fundamental ethical principles apply to one's conduct as a computing professional. Each principle is supplemented by guidelines, which provide explanations to assist members in understanding and applying it. These extraordinary ethical responsibilities of computing professionals are derived from broadly accepted ethical principles.

The Code is not an algorithm for solving ethical problems, rather it is intended to serve as a basis for ethical decision making in the conduct of professional work. Words and phrases in a code of ethics are subject to varying interpretations, and a particular principle may seem to conflict with other principles in specific situations. Questions related to these kinds of conflicts can best be answered by thoughtful consideration of the fundamental ethical principles, understanding the public good is the paramount consideration. The entire profession benefits when the ethical decision making process is transparent to all stakeholders. In addition, it may serve as a basis for judging the merit of a formal complaint pertaining to a violation of professional ethical standards.

1. GENERAL MORAL PRINCIPLES

A computing professional should...

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect diversity. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and privacy. Computing professionals should give consideration to whether the products of their efforts will be used in socially responsible ways, will meet social needs, and will be broadly accessible. They are encouraged to actively contribute to society by engaging in pro bono or volunteer work. When the interests of multiple groups conflict the needs of the least advantaged should be given increased attention and priority.

In addition to a safe social environment, human well-being requires a safe natural environment. Therefore, computing professionals should be alert to, and make others aware of, any potential harm to the local or global environment.

1.2 Avoid harm.
In this document, "harm" means negative consequences to any stakeholder, especially when those consequences are significant and unjust. Examples of harm include unjustified death, unjustified loss of information, and unjustified damage to property, reputation, or the environment. This list is not exhaustive.

Well-intended actions, including those that accomplish assigned duties, may unexpectedly lead to harm. In such an event, those responsible are obligated to undo or mitigate the harm as much as possible. Avoiding unintentional harm begins with careful consideration of potential impacts on all those affected by decisions.

To minimize the possibility of indirectly harming others, computing professionals should follow generally accepted best practices for system design, development, and testing. Additionally, the consequences of emergent systems and data aggregation should be carefully analyzed. Those involved with pervasive or infrastructure systems should also consider Principle 3.7.

At work, a computing professional has an additional obligation to report any signs of system risks that might result in serious personal or social harm. If one's superiors do not act to curtail or mitigate such risks, it may be necessary to "blow the whistle" to reduce potential harm. However, capricious or misguided reporting of risks can itself be harmful. Before reporting risks, the computing professional should thoroughly assess all relevant aspects of the incident as outlined in Principle 2.5.

1.3 Be honest and trustworthy.
Honesty is an essential component of trust. A computing professional should be fair and not make deliberately false or misleading claims and should provide full disclosure of all pertinent system limitations and potential problems. Fabrication of data, falsification of data, and scientific misconduct are similarly violations of the Code. One who is professionally dishonest is accountable for any resulting harm.

A computing professional should be honest about his or her own qualifications, and about any limitations in competence to complete a task. Computing professionals should be forthright about any circumstances that might lead to conflicts of interest or otherwise tend to undermine the independence of their judgment.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member should exercise care not to misrepresent ACM, or positions and policies of ACM or any ACM units.

1.4 Be fair and take action not to discriminate.
The values of equality, tolerance, respect for others, and equal justice govern this principle. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, military status, national origin, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of ACM policy. Sexual harassment is a form of discrimination that limits fair access to the spaces where the harassment takes place.

Inequities between different groups of people may result from the use or misuse of information and technology. Technologies should be as inclusive and accessible as possible. Failure to design for inclusiveness and accessibility may constitute unfair discrimination.

1.5 Respect the work required to produce new ideas, inventions, and other creative and computing artifacts.
The development of new ideas, inventions, and other creative and computing artifacts creates value for society, and those who expend the effort needed for this should expect to gain value from their work. Computing professionals should therefore provide appropriate credit to the creators of ideas or work. This may be in the form of respecting authorship, copyrights, patents, trade secrets, non-disclosure agreements, license agreements, or other methods of attributing credit where it is due.

Both custom and the law recognize that some exceptions to a creator's control of a work are necessary to facilitate the public good. Computing professionals should not unduly oppose reasonable uses of their intellectual works.

Efforts to help others by contributing time and energy to projects that help society illustrate a positive aspect of this principle. Such efforts include free and open source software and other work put into the public domain. Computing professionals should avoid misappropriation of a commons.

1.6 Respect privacy.
"Privacy" is a multi-faceted concept and a computing professional should become conversant in its various definitions and forms.

Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Computing professionals should use personal data only for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals or groups. Computing professionals should establish procedures that allow individuals to review their personal data, correct inaccuracies, and opt out of automatic data collection.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information should be clearly defined and enforced, and personal information gathered for a specific purpose should not be used for other purposes without consent of the individual(s). When data collections are merged, computing professionals should take special care for privacy. Individuals may be readily identifiable when several data collections are merged, even though those individuals are not identifiable in any one of those collections in isolation.

"Privacy" is a multi-facet concept and a computing professional should become conversant in its various definitions and forms.

1.7 Honor confidentiality.
Computing professionals should protect confidentiality unless required to do otherwise by a bona fide requirement of law or by another principle of the Code.

User data observed during the normal duties of system operation and maintenance should be treated with strict confidentiality, except in cases where it is evidence for the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to appropriate authorities, and the computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

2. PROFESSIONAL RESPONSIBILITIES

A practicing computing professional should...

2.1 Strive to achieve the highest quality in both the process and products of professional work.
Computing professionals should insist on high quality work from themselves and from colleagues. This includes respecting the dignity of employers, colleagues, clients, users, and anyone affected either directly or indirectly by the work. High quality process includes an obligation to keep the client or employer properly informed about progress toward completing that project. Professionals should be cognizant of the serious negative consequences that may result from poor quality and should resist any inducements to neglect this responsibility.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.
High quality computing depends on individuals and teams who take personal and organizational responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and awareness of the social context in which the work may be deployed. Professional competence also requires skill in reflective analysis for recognizing and navigating ethical challenges. Upgrading necessary skills should be ongoing and should include independent study, conferences, seminars, and other informal or formal education. Professional organizations, including ACM, are committed to encouraging and facilitating those activities.

2.3 Know, respect, and apply existing laws pertaining to professional work.
ACM members must obey existing regional, national, and international laws unless there is a compelling ethical justification not to do so. Policies and procedures of the organizations in which one participates must also be obeyed, but compliance must be balanced with the recognition that sometimes existing laws and rules are immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

2.4 Accept and provide appropriate professional review.
Quality professional work in computing depends on professional reviewing and critiquing. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical review of the work of others.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computing professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. Extraordinary care should be taken to identify and mitigate potential risks in self-changing systems. Systems whose future risks are unpredictable require frequent reassessment of risk as the system develops or should not be deployed. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in Principle 1.3.

As noted in the guidance for Principle 1.2 on avoiding harm, any signs of danger from systems should be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for Principle 1.2 for more details concerning harm, including the reporting of professional violations.

2.6 Accept only those responsibilities for which you have or can obtain the necessary expertise, and honor those commitments.
A computing professional has a responsibility to evaluate every potential work assignment. If the professional's evaluation reveals that the project is infeasible, or should not be attempted for other reasons, then the professional should disclose this to the employer or client, and decline to attempt the assignment in its current form.

Once it is decided that a project is feasible and advisable, the professional should make a judgment about whether the project is appropriate to the professional's expertise. If the professional does not currently have the expertise necessary to complete the project the professional should disclose this shortcoming to the employer or client. The client or employer may decide to pursue the project with the professional after time for additional training, to pursue the project with someone else who has the required expertise, or to forego the project.

The major underlying principle here is the obligation to accept personal accountability for professional work. The computing professional's ethical judgment should be the final guide in deciding whether to proceed.

2.7 Improve public understanding of computing, related technologies, and their consequences.
Computing professionals have a responsibility to share technical knowledge with the public by creating awareness and encouraging understanding of computing, including the impacts of computer systems, their limitations, their vulnerabilities, and opportunities that they present. This imperative implies an obligation to counter any false views related to computing.

2.8 Access computing and communication resources only when authorized to do so.
This principle derives from Principle 1.2 - "Avoid harm to others." No one should access or use another's computer system, software, or data without permission. One should have appropriate approval before using system resources, unless there is an overriding concern for the public good. To support this clause, a computing professional should take appropriate action to secure resources against unauthorized use. Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with other principles in the Code (such as Principle 1.4).

3. PROFESSIONAL LEADERSHIP PRINCIPLES

In this section, "leader" means any member of an organization or group who has influence, educational responsibilities, or managerial responsibilities. These principles generally apply to organizations and groups, as well as their leaders.

A computing professional acting as a leader should...

3.1 Ensure that the public good is a central concern during all professional computing work.
The needs of people—including users, other people affected directly and

indirectly, customers, and colleagues—should always be a central concern in professional computing. Tasks associated with requirements, design, development, testing, validation, deployment, maintenance, end-of-life processes, and disposal should have the public good as an explicit criterion for quality. Computing professionals should keep this focus no matter which methodologies or techniques they use in their practice.

3.2 Articulate, encourage acceptance of, and evaluate fulfillment of the social responsibilities of members of an organization or group.
Technical organizations and groups affect the public at large, and their leaders should accept responsibilities to society. Organizational procedures and attitudes oriented toward quality, transparency, and the welfare of society will reduce harm to members of the public and raise awareness of the influence of technology in our lives. Therefore, leaders should encourage full participation in meeting social responsibilities and discourage tendencies to do otherwise.

3.3 Manage personnel and resources to design and build systems that enhance the quality of working life.
Leaders are responsible for ensuring that systems enhance, not degrade, the quality of working life. When implementing a system, leaders should consider the personal and professional development, accessibility, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

3.4 Establish appropriate rules for authorized uses of an organization's computing and communication resources and of the information they contain.
Leaders should clearly define appropriate and inappropriate uses of organizational computing resources. These rules should be clearly and effectively communicated to those using their computing resources. In addition, leaders should enforce those rules, and take appropriate action when they are violated.

3.5 Articulate, apply, and support policies that protect the dignity of users and others affected by computing systems and related technologies.
Dignity is the principle that all humans are due respect. This includes the general public's right to autonomy in day-to-day decisions.

Designing or implementing systems that deliberately or inadvertently violate, or tend to enable the violation of, the dignity or autonomy of individuals or groups is ethically unacceptable. Leaders should verify that systems are designed and implemented to protect dignity.

3.6 Create opportunities for members of the organization and group to learn, respect, and be accountable for the principles, limitations, and impacts of systems.
This principle complements Principle 2.7 on public understanding. Educational opportunities are essential to facilitate optimal participation of all organization or group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties, including experiences that familiarize them with the consequences and limitations of particular types of systems. Professionals should know the dangers of oversimplified models, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and the contexts in which they are deployed, and other issues related to the complexity of their profession.

3.7 Recognize when computer systems are becoming integrated into the infrastructure of society, and adopt an appropriate standard of care for those systems and their users.
Organizations and groups occasionally develop systems that become an important part of the infrastructure of society. Their leaders have a responsibility to be good stewards of that commons. Part of that stewardship requires that computing professionals monitor the level of integration of their systems into the infrastructure of society. As the level of adoption changes, there are likely to be changes in the ethical responsibilities of the organization. Leaders of important infrastructure services should provide due process with regard to access to these services. Continual monitoring of how society is using a product will allow the organization to remain consistent with their ethical obligations outlined in the principles of the code. Where such standards of care do not exist, there may be a duty to develop them.

4. COMPLIANCE WITH THE CODE

A computing professional should...

4.1 Uphold, promote, and respect the principles of the Code.
The future of computing depends on both technical and ethical excellence. Computing professionals should adhere to the principles expressed in the Code. Each ACM member should encourage and support adherence by all computing professionals. Computing professionals who recognize breaches of the Code should take whatever actions are within their power to resolve the ethical issues they recognize.

4.2 Treat violations of the Code as inconsistent with membership in ACM.
If an ACM member does not follow the Code, membership in ACM may be terminated.

Join the Discussion

The Committee on Professional Ethics is asking you to participate in an open discussion about this Code and suggest ways in which it might be improved: **http://code2018.acm.org/discuss**; **https://ethics.acm.org**; or by direct email to **chair@ethics.acm.org**.

Bo Brinkman (bo.brinkman@miamioh.edu) is an associate professor of computer science and software engineering at Miami University, Oxford, OH.

Catherine Flick (cflick@dmu.ac.uk) is a Senior Lecturer in Computing and Social Responsibility at De Montfort University, Leicester, UK.

Don Gotterbarn (gotterbarn@acm.org) is chair of the ACM Committee on Professional Ethics and Professor Emeritus in the Department of Computing at East Tennessee State University, Johnson City.

Keith Miller (millerkei@umsl.edu) is the Orthwein Endowed Professor for Lifelong Learning in the Sciences College of Education, University of Missouri, St. Louis.

Kate Vazansky (kate.vazansky@gmail.com) is a Technical Program Manager at Salesforce.

Marty J. Wolf (mjwolf@acm.org) is a professor of computer science at Bemidji State University, Bemidji, MN.